UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/769,038	01/30/2004	Daniel M. Bodorin	13768.1308	7942

47973 7590 10/12/2010

WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CTY, UT 84111

EXAMINER	
ARMOUCHE, HADI S	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
10/12/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/769,038	BODORIN ET AL.	
	Examiner	Art Unit	
	HADI ARMOUCHE	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 September 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,7,13 and 16-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,7,13 and 16-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *04/01/2010*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 09/20/2010 has been entered.

2. Claims 1-4, 7, 13 and 16 have been amended; claims 5-6, 8-12, 14-15 and 19-20 have been cancelled. Claims 1-4, 7, 13 and 16-18 remain pending.

Response to Arguments

3. Acknowledgment to applicant's amendment to the specification has been noted. The specification has been reviewed, entered and found obviating to previously raised objection for minor informality.

4. Applicant's cancellation to claims 14, 15 and 20 renders claim rejection to claims 14, 15 and 20 under 35 U.S.C 101 moot. Rejection to claims 14, 15 and 20 under 35 U.S.C 101 is hereby withdrawn.

5. Applicant's amendment to the specification on 09/20/2010 obviates previously raised rejection to claims 4 and 16 under 35 U.S.C 101. Rejection under 35 U.S.C 101 is hereby withdrawn.

6. Applicant's arguments with respect to claims 1-4, 7, 13 and 16-18 have been considered but are not persuasive in view of the new ground(s) of rejection necessitated by the amendment to the claims

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-4, 7, 13 and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over White et al. ("Anatomy of a Commercial-Grade Immune System", http://citeseer.ist.psu.edu/white99anatomy.html, 1999), hereafter "White" in view of Schultz et al. (US 2003/0065926) referred to hereinafter by Schultz in further in view of Muttik et al. (US 2004/0199827) to hereinafter by Muttik.

9. Regarding claim 1, White discloses a malware detection system and means for determining whether a code module is malware according to the code module's exhibited behaviors (Fig. 3, page 14), the system comprising a memory storing the following computer executable components:

at least one dynamic behavior evaluation module (Fig. 6, page 20, Analysis Center reads on dynamic behavior evaluation module), wherein each dynamic behavior evaluation module provides a virtual environment for executing a code module of a particular type (Section "Creation of the replication environment", Page 20: paragraph 1: lines 1-5), and wherein each dynamic behavior evaluation module

records execution behaviors of the code module makes as it is executed, wherein a behaviors of the code module are recorded into a behavior signature corresponding to the code module: (Fig. 6, page 20: item "archive" and Section "Analysis", page 21: paragraph 1: lines 5-6, extract good signature and stores in the archive for developing virus definition reads on each dynamic behavior evaluation module records some behaviors which may be exhibited by the code module as it is executed into a behavior signature);

a management module, wherein the management module obtains the code module, and wherein the management module evaluates the code module to determine the code module's type (page 23 under "Scaling the analysis center" 1st paragraph and page 25 under "Macro Viruses: 1st paragraph) , and wherein the management module selects a dynamic behavior evaluation module to execute the code module according to the code module's type (Fig. 6: page 20: item "workflow supervisor" and Section "Macro Viruses": page 25: paragraph 1: lines 5-7, supervisor accept suspected virus sample and feed into different virtual environment for each format and language of Macro Virus reads on a management module for obtaining the code module and selecting a dynamic behavior evaluation module to execute the code module according to the code module's type);

a malware behavior signature store storing at least one known malware behavior signature of a known malware (Fig. 3: item archive, Page 20, and Section "The Supervisor" pages 18 and 19, paragraph 3: lines 1-2 and Section "Definition generation", Page 21: paragraph 1: lines 1-10, archive and virus definition file reads

on malware behavior signature store storing at least one known malware behavior signature);

a behavior signature comparison module that obtains the behavior signature of the code module and compares the behavior signature of the code module to the known malware behavior signatures in the malware behavior signature store to determine whether the behaviors recorded in the behavior signature of the code module match behaviors recorded in a behavior signature of a known malware (Section "An active network to Handle Epidemics and Floods – Over view", pages 13-15: paragraph 5: lines 1-2, gateway scans the sample file against the latest virus definition reads on a behavior signature comparison module that obtains the behavior signature and compares the behavior signature to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited behaviors of the code module match the exhibited behaviors of known malware and page 18 2nd paragraph and page 20 first paragraph);

Even though White teaches that the malware detection system is configured to report whether the code module is malware or not (Section "An active network to Handle Epidemics and Floods – Over view", pages 13-15), White does not explicitly teaches that the malware detection system is configured to report whether the code module is malware based at least in part of the degree that the behaviors recorded in the behavior signature of the code module match behaviors recorded in a behavior signature of the known malware.

Schultz teaches that the malware detection system is configured to report whether the code module (executable) is malware based at least in part of the degree (probability or likelihood) that the code module's exhibited execution behaviors match the exhibited behaviors of a known malware [abstract last 8 lines and paragraph 0022].

At the time of the invention was made, it would have been obvious to an ordinary skill in the art to combine Schultz's teachings in White's system. The motivation/suggestion would have been to make the system for reliable and secure by detecting malicious executables [Schultz, paragraph 0005].

The combined teachings of White and Schultz do not explicitly teach that the execution behaviors are interesting API function calls wherein the interesting API function calls are specified by a user and comprise a portion of all API function calls that the code module makes, wherein only the interesting API function calls, but not all the API function calls, that the code module makes during execution in the dynamic behavior evaluation module are recorded. Muttik teaches that the execution behaviors are interesting API function calls wherein the interesting API function calls are specified by a user and comprise a portion of all API function calls that the code module makes, wherein only the interesting API function calls, but not all the API function calls, that the code module makes during execution in the dynamic behavior evaluation module are recorded [paragraphs 0037, 0038, 0040 and 0041].

At the time of the invention was made, it would have been obvious to an ordinary skill in the art to modify the combined method of White and Schultz with Muttik's teachings. The motivation/suggestion would have been to be able to identify the source code of the malware [Muttik, abstract].

10. The system of claim 2, the method of claim 3 and the computer-readable medium of claim 4 have the same limitations as claim 1 and hence same rejection rational is applied.

11. For claim 7 and similar claims 10, 13 and 16, White discloses wherein the predefined set of execution behaviors to record corresponds to a set of system calls (page 20, paragraph 1 "classification".

12. For claim 17 and similar claim 18, White discloses wherein the malware detection system is further configured to report a positive identification of a known malware (Section "An active network to Handle Epidemics and Floods – Over view", pages 13-15: paragraph 5: lines 1-2, gateway scans the sample file against the latest virus definition reads on a behavior signature comparison module that obtains the behavior signature and compares the behavior signature to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited behaviors of the code module match the exhibited behaviors of known malware).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HADI ARMOUCHE whose telephone number is

(571)270-3618. The examiner can normally be reached on M-Th 7:30-5:00 and Fridays half day.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/H. A./
HADI ARMOUCHE
Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432